What is claimed is:

1. A method for calculating a One Time Password, comprising:

concatenating a secret with a count, where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated at the token and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password;

calculating a hash based upon the concatenated secret and count; and

truncating the result of the hash to obtain a One Time Password.

2. A method for authenticating a request for access to a resource, comprising:

receiving at an authentication server a request for authentication that includes a serial number that is uniquely associated with a token, a personal identification number associated with a user and a One Time Password generated at a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server;

retrieving at the authentication server the value of a count that corresponds to the token based upon the serial number;

retrieving at the authentication server the secret that corresponds to the token based upon the serial number;

calculating at the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

comparing the calculated One Time Password with the received One Time Password; and

if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated;

if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count

and the secret, and comparing the recalculated One Time Password with the received One Time Password;

if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password.

3. The method of claim 2, wherein the hash function is SHA-1.

4. The method of claim 2, wherein the secret is a symmetric cryptographic key.

5. The method of claim 2, wherein incrementing the count and recalculating the One Time Password is repeated a predetermined number of times, and if the recalculated One Time Password does not correspond to the received One Time Password by the end of the predetermined number of times, the request is determined to be not authenticated.

6. A method for authenticating a request for access to a resource, comprising:

receiving at an authentication server a request for authentication that includes a username that is uniquely associated with a user, a personal identification number associated with a user and a One Time Password generated at a token, wherein the One Time Password is based upon the value of a count at the token and a secret shared between the token and the authentication server;

retrieving at the authentication server the value of a count that corresponds to the token based upon the username;

retrieving at the authentication server the secret that corresponds to the token based upon the username;

calculating at the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

comparing the calculated One Time Password with the received One Time Password; and

if the calculated One Time Password corresponds to the received One Time Password, the request is determined to be authenticated;

if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password;

if the recalculated One Time Password does not correspond to the received One Time Password, then repeating to increment the count and to recalculate the One Time Password until the recalculated One Time Password corresponds to the received One Time Password.

7. The method of claim 6, wherein the hash function is SHA-1.

8. The method of claim 6, wherein the secret is a symmetric cryptographic key.

9. The method of claim 6, wherein incrementing the count and recalculating the One Time Password is repeated a predetermined number of times, and if the recalculated One Time Password does not correspond to the received One Time Password by the end of the predetermined number of times, the request is determined to be not authenticated.